

计算机网络信息安全中数据加密技术的分析

朱平哲

(三门峡职业技术学院, 河南 三门峡 472000)

摘要:随着科技水平的不断发展,计算机技术的逐渐进步,世界已经进入了信息化时代。世界各地对计算机的使用已经趋向于平民化,计算机技术逐渐被广大群众所重视并需要。与此同时,关于计算机网络信息安全中出现的信息安全问题,也越来越多,这直接影响着广大群众的信息安全。计算机网络信息安全中数据加密技术的探索与研究,成为众多科研人员所关注的重点问题。本文就计算机网络信息安全中数据加密技术的相关内容,进行了一个分析。

关键词:计算机网络信息安全;数据加密技术;安全问题;实际应用

中图分类号:TP393 **文献标识码:**A

文章编号:1009-3044(2019)36-0024-02

DOI:10.14004/j.cnki.ckt.2019.4267



开放科学(资源服务)标识码(OSID):

21 世纪是一个科技发达的时代,是一个以网络信息技术为主导的信息时代。尤其是因为近些年计算机技术的快速发展,结合互联网的迅速发展,计算机与互联网已经成为群众生活中所不可缺少的东西。在几乎所有人都在使用计算机网络的情况下,相对地出现了一些信息安全的问题,这时刻影响着广大群众的信息安全。数据加密技术的出现,其目的就是为了解决这一重大问题。数据加密技术地使用,也很好地解决了信息安全的问题,在很大程度上,保障了广大群众的信息数据的安全。

1 计算机网络信息安全

计算机网络信息安全,就是指人们在使用计算机进行网络运行的时候,即使用电脑上网的时候,直接的利用互联网的管理技术,来保证上网时的网络环境的安全性,保证网络正常安全的运行,尤其是网络数据的安全,保证群众上网时的信息数据的完整与安全,实现信息数据的保密性。

也因此,计算机网络信息安全具有完整性、可审查性、可使用性以及保密性的特点。完整性,就是指用户在使用计算机进行网络运行的时候,能够很好地保证使用者在网络中输入以及储存的信息的完整,保证用户所有的信息不被破坏或修改,确保网络信息的完整性。可审查性,就是指用户在使用计算机的时候,如果发现自己的网络信息出现安全问题,如泄露、毁坏等情况,在保证使用者合理使用需求的情况下,用户有权查询自己的网络信息。可使用性,就是指用户在使用计算机的时候,在计算机中所储存的网络信息,用户有权使用,在用户需要的时候,可以随时使用自己的网络信息。保密性,就是指用户在使用计算的时候,在计算机中储存的所有网络信息,都属于用户自己的隐私,这些网络信息具有保密性,不经过用户的同意不能被其他人查看或使用。

2 数据加密技术及其不同的类别

2.1 数据加密技术

数据加密技术,就是指以计算机为技术的系统载体,利用

加密密钥和各种不同的算法等技术,结合网络信息的重组,将数据与信息进行合理的加密,来保证网络信息安全的技术。基础的表现,就是在对数据进行加密的时候,因算法的作用,将数据信息转化成密文,在需要使用这些网络信息的时候,需要使用密钥才能完整的、正确的获得相对应的密文信息,在很大程度上,保障了网络信息数据的安全。

2.2 数据加密技术不同的类别

在使用数据加密技术对网络信息数据进行保护使用的时候,最基础的密钥算法就是对称密钥与非对称密钥的使用。对称密钥,就是指使用相同的一个密钥,可以同时通过网络信息数据进行加密和解密。非对称密钥,与对称密钥刚好相反,就是在进行网络信息数据加密与解密的过程中,需要使用不同的密钥来处理。也因为不同的算法,会产生不同种类的数据加密技术,接下来我们来简单地了解一下比较常见的几种数据加密技术。

2.2.1 端端加密技术

端端加密技术,就是指在传递数据前,对信息数据进行加密,直接传递相对应的密文数据,接收方接收到密文后,再使用相对应的密钥对接收的密文进行解密,从而获得需要的数据信息。端端加密技术的优点是使用的价格相对便宜,物美价廉。而且,数据在传递的时候,是两端进行加密、解密,更好地保证了信息数据的安全性。

2.2.2 节点加密技术

节点加密技术,就是指借助链路为技术的载体,通过每一个节点,对要传递的信息数据进行加密与解密。然而,虽然在通信的节点处,会有一个相对安全的区域,而且信息数据也是以密文的形式进行传递的,但是数据加密与解密的过程中,是在各自的安全区域内进行的,相对而言过于简单,容易被别人破解,获得密文背后的信息数据。

收稿日期:2019-06-21

基金项目:2015 年度河南省教育厅科学技术研究重点项目:基于嵌入式 Linux 的家庭智能系统的设计及关键技术研究(15B520026)

作者简介:朱平哲(1982—),女,河南驻马店人,讲师,硕士研究生,研究方向为计算机数据库、图形学。

2.2.3 链路加密技术

链路加密技术,顾名思义,也是以链路为载体,信息数据在进行传递的时候,也是以密文的形式进行传递的,而且在信息传递的过程中,信息数据会进行反复的加密与解密,并且这个过程覆盖了整个传输路径之中,相对于节点加密技术,更具有安全性,对信息数据的安全保护作用也更好。

3 计算机网络信息存在的安全问题

数据加密技术出现的最直接的原因,是因为用户在使用计算机的时候,尤其是在进行信息数据储存过程中或是信息数据使用的时候,会因为一些不好的因素,而出现信息泄露、丢失的问题。这给用户带来了很大的困扰,甚至有可能给用户带来一定的经济损失。因此,数据加密技术的出现和使用,成为对用户的信息数据以及利益进行保护的关键。

3.1 计算机系统配置带来的安全问题

计算机的系统配置,对于用户的信息数据的安全,有着很大的影响。有些计算机的系统中,所自带的防火墙的配置过低,防护效果非常不好,再加上杀毒软件等安全措施做得不够,就会产生很大的信息数据的安全问题。尤其是一些计算机,因为防火墙与杀毒软件等保护措施,版本和配置相对过于低下,根本不能够满足计算机自身系统配置运行的要求。再加上计算机操作系统的短板问题,主要体现在计算机通信协议、网络浏览器、超级用户的使用等漏洞问题。操作系统是计算机传递信息的载体,如果出现问题,就很容易导致用户在使用计算机的时候,出现信息安全问题。

3.2 病毒带来的安全问题

用户在使用计算机的时候,最容易遇到的就是病毒带来的安全的问题。病毒已经成为当下计算机使用的首要安全问题之一,病毒不仅有着许多不同的种类,而且其传播的速度还非常的快,传播的方式也多种多样。最重要的是,病毒的危害性可以说是非常的强。如果用户在使用计算机的时候,因为计算机的网络安全防护问题,或是自己的操作问题,导致病毒在用户使用计算机的时候,传播在电脑里,就会导致用户的信息数据出现泄露或丢失的情况,给用户的信息数据安全带来很大的威胁与损害,甚至给用户带来不可忽视的经济损失。

3.3 黑客带来的安全问题

除了计算机系统的配置问题以及病毒问题,在当下的网络环境中,最让用户担心与害怕的,就是黑客所带来的安全问题。在现在的网络环境中,会有一些计算机技术非常高超,但又心怀不轨的不法分子,通过使用自身的计算机技术,针对别人的计算机,进行目的性的恶意攻击,导致受众的计算机出现系统故障等问题。有些黑客甚至会通过攻击别人的计算机,来获得他人计算机内的信息数据,或是对他人计算机内的信息进行更改、盗用等。更有甚者,会使用黑客技术随意的攻击别人,给别人带来困扰。这些黑客的所作所为,不仅给其他用户带来严重的信息数据的安全威胁,还可能会产生很严重的经济损失。

3.4 用户自己操作不当带来的安全问题

当然,还有一个最简单、直接的原因,就是用户自己的操作不当,所带来的安全问题。虽然现象计算机已经相对普及了,几乎每一个民众都会使用计算机进行网络操作。然而,真正懂得、了解计算机的人,却只是一部分人。有很多用户只是懂得

计算机的简单使用,导致在使用过程中,出现一些操作不当的问题。比如有的用户不了解防火墙的作用,甚至认为防火墙没有作用,而做出卸载防火墙的事情,这就导致计算机的系统出现安全隐患,很容易造成信息数据出现泄露或丢失的安全问题。再比如有些用户在使用计算机的时候,访问一些不安全、不健康的网站,甚至访问一些存在病毒等安全隐患的网站,导致计算机出现故障问题,给自己的网络信息数据带来安全问题。

4 计算机网络信息安全中数据加密技术的实际应用

为了减少用户在使用计算机过程中,出现的一系列影响信息数据安全问题,减轻因信息泄露或丢失而产生的损失。将数据加密技术实际的应用到计算机网络中,就必不可少了。通过对数据加密技术的使用,来直接的保护用户的信息数据,保障用户在使用计算机时候的信息安全。

4.1 数据加密技术在数据库中的应用

数据库应用的安全,关乎着当下许多计算机用户的信息安全。尤其是单以数据库本身而言,虽然有着一定的安全措施,但是其自身的防护措施的级别却是很低,很难对用户的信息数据进行保护。也因此,数据加密技术就被用于数据库的信息保护之中。这样一来,当用户使用计算机的时候,如果需要在数据库中使用相应的信息,就可以进行针对性选择以及解密,获取自己需要的信息。而且,在信息传递或是储存过程中,如果信息泄露,不法分子在没有解密密钥的情况下,也无法直接了解信息的实际内容,这就很好地保证了用户的信息数据的安全。在结合对数据库使用数据加密技术的同时,对计算机进行安装合适的防火墙,针对计算机的实际配置,搭配合理的防火墙系统,这样在计算机出现安全异常的时候,能够进行及时的拦截,进一步的保证数据库的安全与稳定,保证用户的信息数据的安全。

4.2 数据加密技术在软件程序中的应用

我们在使用计算机的时候,主要就是依靠对各种不同作用的软件的使用,来满足自己对计算机的使用目的。而无论我们是在计算机中储存的自己的信息数据,还是在使用各种软件的过程中,产生的众多数据,在进行计算机使用的时候,就很容易受到病毒和黑客的影响,导致用户的信息数据出现安全问题。数据加密技术在软件程序中的应用,主要就体现在杀毒软件的使用。杀毒软件本身,就是利用数据加密技术而制定了一定的防查程序,用户通过杀毒软件的应用,对计算机进行不定期的排查,对出现的所有可能危害用户信息数据安全的因素,进行处理、调整,来保障计算机的正常使用以及用户的信息数据安全。同时,在使用软件的过程中,尤其是一些如QQ、微信、邮箱等传递信息的软件,可以利用数据加密技术中的节点加密技术、端端加密技术或是链路加密技术等,对传递的信息进行实时的保护,做好信息数据的加密、解密工作,保障用户信息数据的安全。

4.3 数据加密技术在电子商务中的应用

近年来,随着网络技术的发展,电子商务成为社会上的主流商务交易形式,各种电子交易平台纷纷出现,用户也非常喜欢这种简单便捷的交易方式。然而,用户在进行电子商务交易的时候,无论是买家还是卖家,都需要提供一定的个人信息。

(下转第32页)

统,对网络攻击进行实时诱捕,感知系统安全状况。部署入侵检测系统,建立垃圾邮件过滤系统方案。

3.2 终端设备层面

在终端计算机上部署安全专业的云服务,及时安装系统安全漏洞补丁、防恶意程序软件、杀毒软件、主机网络防火墙软件等,及时做好软件升级和打补丁工作。在终端计算机上设置无规律的强密码(至少12位,同时包含数字、大写字母、小写字母、特殊字符三种以上)作为系统登录密码,并且强制要求每台服务器使用不同的密码进行管理。尽量关闭不必要的端口或服务,如关闭Windows共享服务、远程桌面控制等,如对共享服务确有需要的,必须使用访问控制列表和强密码保护来限制访问权限,禁用对共享文件夹的匿名访问。不要随意打开来源不明的文档、网络链接和邮件附件等,不乱插移动存储设备。

3.3 数据审计层面

数据安全方面,保护好重要的文档。内网核心业务区要加强数据存储加密、数据的备份与恢复的建设,实时备份系统重要数据到异地存储介质中,对必须要保存到本地的重要文档进行加密存储。并在核心业务区部署数据库审计系统、服务器群组防护系统,实现对数据库登录账号、登录工具、系统漏洞、服务器接入控制和数据操作过程等的跟踪及实时监测,并能够智能地分析、还原各种数据库操作过程,确保实现各接入点医疗信息数据可靠、传输数据有源可溯,安全事件预警等功能。

3.4 应急响应层面

在管理中心成立响应中心和安全事件管理中心,配备信息安全技术人员,定期对网络、系统、设备等做安全检测,根据检测情况配备安全产品、部署安全防护。定期对医疗系统工作人员进行安全培训,提高他们的网络安全意识。

一旦检测到有病毒入侵,应立即断开已经感染的主机系统的网络连接,防止进一步扩散。针对已经感染终端,根据终端数据重要性决定处置方式,采用数据恢复软件、磁盘硬件数据恢复服务进行数据恢复,尽可能减小数据损失。针对需要重新安装系统则建议完全格式化硬盘、重建磁盘引导扇区后,安装全新操作系统,并完善操作系统补丁、安装防病毒软件并通过检查确认无相关漏洞后再恢复网络连接。

4 结束语

病毒防范是一项长期、持久的工作,需要医疗系统全员的参与,只有提高网络安全意识、加强设备规范操作、完善网络安全建设,才能有效构建一个医疗行业的网络安全壁垒。

参考文献:

- [1] 叶梦娇.企业中防病毒系统的应用及发展[J].网络安全技术与应用,2015(5):44,46.
- [2] 汪余宏.企业网络防病毒解决方案与实践[J].计算机时代,2013(7):24-27.

【通联编辑:朱宝贵】

(上接第25页)

比如身份证、联系方式、地址、银行卡号等,甚至在交易的时候,还需要提供支付密码等信息。这些信息完全属于用户的隐私信息,跟用户的切身利益息息相关,如果在进行交易的时候,这些信息因为一些原因而泄露了出去,势必会给用户带来不可忽视的损失。也因此,很多电商平台为了保护自身以及客户的切实利益,会使用安全证书、数字签名、SSL和SET等数据加密技术,对客户的信息使用设置一定的权限,让客户在交易的时候,需要进行信息审核等操作,对客户的隐私信息,进行全方位的保护,避免客户出现利益损失的问题。

4.4 数据加密技术在虚拟专用网络中的应用

虚拟专用网络,是在信息技术快速发展的前提下,满足广大群众上网需要的产物。虚拟专用网络,是计算机的网络系统中,一个非常重要的组成部分,在当下网络环境中,最直接的体现就是路由器网络,也是当下许多群众所喜欢使用的一种上网方式,网络信息的数据安全问题十分重要。虚拟专用网络对于数据加密技术的使用,也就是通过路由器,对VPN数据进行一个系统的加密,将各区域的网络进行一个串联,进行网络信息数据传递的时候,对信息数据进行自动的加密,保证信息数据的安全。从而,保证用户在使用路由器的无线网络,进行网络

信息传递的时候,保障用户的信息安全以及利益安全。

5 结束语

综上所述,本文主要就是针对计算机网络信息安全中数据加密技术的使用进行的一系列的分析。通过对网络信息安全以及数据加密技术的了解,以及对计算机网络信息安全存在的安全问题的了解,直接的分析数据加密技术在计算机网络信息安全中的实际应用。尤其是体现数据加密技术在保护用户的隐私信息以及信息数据的安全方面的作用,希望通过本文的分析研究,能够帮助用户更好地保护自己的计算机的安全,尤其是自己的信息数据的安全,保证自己的数据不会出现信息泄露或是丢失的问题,保障自己的切身利益不受损害。

参考文献:

- [1] 宋初.数据加密技术在计算机网络通信安全中的应用与分析[J].网络安全技术与应用,2018(7).
- [2] 陈智松.数据加密技术在计算机网络通信安全中的应用[J].智库时代,2018(47).
- [3] 王晓楠,周婧.计算机网络通信安全中数据加密技术的应用[J].计算机产品与流通,2018(12).

【通联编辑:唐一东】